

10-2-00

A



Please type a plus sign (+) inside this box PTO/SB/05 (12/97)

Approved for use through 09/30/00. OMB 0651-0032

Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No. 042390.P9007 Total Pages 26

First Named Inventor or Application Identifier Jesse R. Walker

Express Mail Label No. EL627467053US

ADDRESS TO: **Commissioner of Patents & Trademarks**
Box Patent Application
Washington, D. C. 20231

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

1. Fee Transmittal Form
(Submit an original, and a duplicate for fee processing)
2. Specification **(Total Pages 26)**
(preferred arrangement set forth below)
 - Descriptive Title of the Invention
 - Cross References to Related Applications
 - Statement Regarding Fed sponsored R & D
 - Reference to Microfiche Appendix
 - Background of the Invention
 - Brief Summary of the Invention
 - Brief Description of the Drawings (if filed)
 - Detailed Description
 - Claims
 - Abstract of the Disclosure
3. Drawings(s) 9 (35 USC 113) **(Total Sheets 6)**
4. Oath or Declaration **(Total Pages 6)**
 - a. Newly Executed (Original)
 - b. Copy from a Prior Application (37 CFR 1.63(d))
(for Continuation/Divisional with Box 17 completed) **(Note Box 5 below)**
 - i. **DELETIONS OF INVENTOR(S)** Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
5. Incorporation By Reference (useable if Box 4b is checked)
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

6. Microfiche Computer Program (Appendix)

7. Nucleotide and/or Amino Acid Sequence Submission
(if applicable, all necessary)

- a. Computer Readable Copy
- b. Paper Copy (identical to computer copy)
- c. Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

8. Assignment Papers (cover sheet & documents(s))

- a. 37 CFR 3.73(b) Statement (where there is an assignee)
- b. Power of Attorney

10. English Translation Document (if applicable)

- 11. a. Information Disclosure Statement (IDS)/PTO-1449
- b. Copies of IDS Citations

12. Preliminary Amendment

13. Return Receipt Postcard (MPEP 503) (Should be specifically itemized)

- 14. a. Small Entity Statement(s)
- b. Statement filed in prior application, Status still proper and desired

15. Certified Copy of Priority Document(s) (if foreign priority is claimed)

16. Other: _____

17. If a **CONTINUING APPLICATION**, check appropriate box and supply the requisite information:

Continuation Divisional Continuation-in-part (CIP)

of prior application No: _____

18. **Correspondence Address**

Customer Number or Bar Code Label 008791
(Insert Customer No. or Attach Bar Code Label here)
or

Correspondence Address Below

NAME Edwin H. Taylor, Reg. No. 25,129

ADDRESS BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

12400 Wilshire Boulevard, Seventh Floor

CITY Los Angeles STATE California ZIP CODE 90025-1026

Country U.S.A. TELEPHONE (408) 720-8300 FAX (408) 720-9397

12/01/97

- 2 -

PTO/SB/05 (12/97)

Approved for use through 09/30/00. OMB 0651-0032
Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

FEE TRANSMITTAL FOR FY 2000**TOTAL AMOUNT OF PAYMENT (\$)768.00****Complete if Known:**Application No. UnknownFiling Date HerewithFirst Named Inventor: Jesse R. WalkerGroup Art Unit UnknownExaminer Name UnknownAttorney Docket No. 042390.P9007**METHOD OF PAYMENT** (check one)

1. The Commissioner is hereby authorized to charge indicated fees and credit any over payments to:

Deposit Account Number 02-2666Deposit Account Name BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP

- Charge Any Additional Fee Required Under 37 CFR 1.16 and 1.17

2. Payment Enclosed:

 Check Money Order Other**FEE CALCULATION****1. BASIC FILING FEE**

Large Entity	Small Entity			
Fee	Fee	Fee	Fee	Fee Paid
Code	(\$)	Code	(\$)	
101	690	201	345	Utility application filing fee 690.00
106	310	206	155	Design application filing fee
107	480	207	240	Plant filing fee
108	690	208	345	Reissue filing fee
114	150	214	75	Provisional application filing fee

SUBTOTAL (1) \$690.00**2. EXTRA CLAIM FEES**

	Extra Claims		Fee from below		Fee Paid
Total Claims 21	- 20** = 00	X	18.00	= 00	
Independent Claims 4	- 3** = 1	X	78.00	= 78.00	
Multiple Dependent				=	

**Or number previously paid, if greater; For Reissues, see below.

Large Entity**Small Entity**

Fee	Fee	Fee	Fee	Fee Description
Code	(\$)	Code	(\$)	
103	18	203	9	Claims in excess of 20
102	78	202	39	Independent claims in excess of 3
104	260	204	130	Multiple dependent claim, if not paid
109	78	209	39	**Reissue independent claims over original patent
110	18	210	9	**Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) \$768.00

FEE CALCULATION (continued)

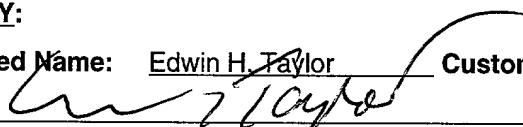
3. ADDITIONAL FEES

<u>Large Entity</u>	<u>Small Entity</u>	<u>Fee Description</u>	<u>Fee Paid</u>
Fee Code	Fee (\$)	Fee Code (\$)	
105	130	205	65
127	50	227	25
139	130	139	130
147	2,520	147	2,520
112	920*	112	920*
113	1,840*	113	1,840*
115	110	215	55
116	380	216	190
117	870	217	435
118	1,360	218	680
128	1,850	228	925
119	300	219	150
120	300	220	150
121	260	221	130
138	1,510	138	1,510
140	110	240	55
141	1,210	241	605
142	1,210	242	605
143	430	243	215
144	580	244	290
122	130	122	130
123	50	123	50
126	240	126	240
581	40	581	40
146	690	246	345
149	690	249	345
Other fee (specify)			
Other fee (specify)			

SUBTOTAL (3) \$ 768.00

*Reduced by Basic Filing Fee Paid

SUBMITTED BY:

Typed or Printed Name:	Edwin H. Taylor	Customer Number:	008791
Signature		Date	September 28, 2000
Reg. Number	25,129	Deposit Account User ID	(complete if applicable)

UNITED STATES PATENT APPLICATION

for

TECHNIQUE TO ESTABLISH WIRELESS SESSION KEYS
SUITABLE FOR ROAMING

Inventor:
Jesse R. Walker

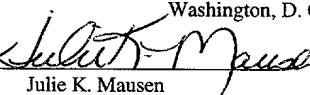
File No: 42390.P9007

Prepared by:
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN
12400 Wilshire Boulevard
Los Angeles, CA 90025-1026
(408) 720-8598

EXPRESS MAIL CERTIFICATE OF MAILING

"Express Mail" mailing label number EL627467053US Date of Deposit September 28, 2000
I hereby certify that I am causing this paper or fee to be deposited with the United States Postal Service "Express Mail Post
Office to Addressee" service on the date indicated above and that this paper or fee has been addressed to:

Box Patent Application
Commissioner of Patents
& Trademarks
Washington, D. C. 20231

Signed by  Date Signed: September 28, 2000
Julie K. Mausen

**TECHNIQUE TO ESTABLISH WIRELESS SESSION
KEYS SUITABLE FOR ROAMING**

FIELD OF THE INVENTION

- 5 This invention relates to authentication technologies generally and particularly to authentication techniques in a wireless network.

BACKGROUND OF THE INVENTION

- A wireless network is a flexible data communication medium implemented as an extension for, or as an alternative to, a wired network. By using radio 10 frequency (RF) technology, wireless networks transmit and receive data over air, minimizing the need and the cost typically associated with wired connections. Moreover, wireless networks offer mobility and flexibility for users. For example, doctors and nurses in hospitals are able to use hand-held devices or notebook computers to access patient information from a server through wireless networks 15 without having to search for a physical jack to plug their devices or computers into.

Figure 1 demonstrates a prior art wireless network configuration. Specifically, the network configuration comprises wireless stations 108 and 110, wireless medium 106 and access points 100, 102 and 104. Wireless stations 108 and 110 communicate with access points 100, 102 and 104 through electromagnetic 20 airwaves 106. Access points 100, 102 and 104 are also connected to wired network 112 and have access to the network resources of wired network 112 such as, server

114, network printer 116 or other devices coupled to wired network 112. It should
be noted that wireless stations 108 and 110 are not stationary and do not have to
communicate with particular multiple access points. For instance, wireless station
108 may seamlessly move from the coverage area of access point 100 to the
5 coverage area of access point 104 and still maintain its data connections with the
access points.

Despite the portability and the convenience that wireless technology offers,
there still lacks a comprehensive security scheme to ensure privacy and integrity of
the data on wireless networks. For instance, one existing approach is to utilize static
10 keys to encrypt data on a wireless link. Such encrypted data are vulnerable to attack,
because the probability of deciphering them is much greater than if the data were
encrypted with constantly changing keys. Another approach involves a wireless
station sharing a group key with an access point. Thus, when any one device on a
wireless network falls into the hands of an attacker, the security of every system in
15 the network is compromised. Yet another approach has every wireless station share
one key. As a result, any wireless station is capable of decrypting the traffic of any
other wireless.

As has been demonstrated, an improved method and an apparatus are needed
to enhance the security of a wireless network.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is illustrated by way of example and is not limited by the figures of the accompanying drawings, in which like references indicate similar elements, and in which:

- 5 **Figure 1** illustrates a prior art wireless network configuration.
- Figure 2** illustrates one embodiment of the present invention, a secured wireless roaming system.
- Figure 3(a)** illustrates a block diagram of one embodiment of a wireless station in accordance with the present invention.
- 10 **Figure 3(b)** illustrates a block diagram of one embodiment of an access point in accordance with the present invention.
- Figure 4** illustrates a flow chart of one process that one embodiment of a wireless station in accordance with the present invention follows.
- Figure 5** illustrates a flow chart of one process that one embodiment of an access point in accordance with the present invention follows.

DETAILED DESCRIPTION

A method and an apparatus for establishing secured roaming are disclosed.

In the following description, numerous specific details are set forth, such as

Kerberos protocol, etc. in order to provide a thorough understanding of the present

5 invention. However, it will be apparent to one of ordinary skill in the art that the
invention may be practiced without these particular details. In other instances, well-known elements and theories such as cryptography systems, etc. have not been
discussed in special details in order to avoid obscuring the present invention.

In addition, the term, “wireless station”, is used throughout the following

10 discussion to refer to any network device that uses some wireless Local Area
Network (hereinafter LAN) technology to communicate with a wired network. It
can be either an end system or a switching element. Also, a “secured” session refers
to information exchanges between two networking devices, where some form of
security measures safeguard such exchanges. A “replay attack” describes one form
15 of an attack on a security system. Specifically, a perpetrator who launches such an
attack intercepts messages destined for a recipient and replays those intercepted
messages back to the recipient.

Unless specifically stated otherwise, the term, “Kerberos protocol”, refers to

Kerberos Version 5, released on May 5, 1995. It is an authentication protocol that
20 allows entities to authenticate their identities to one another over physically insecure

networks and at the same time still prevents eavesdropping and replay attacks. It also incorporates cryptography systems to further provide for data stream integrity (such as detection of modification) and secrecy (such as preventing authorized reading). The Kerberos protocol operates within the Kerberos infrastructure, which

5 comprises, but not limited to, the following:

- 1) Key Distribution Center (KDC): maintains and controls the distribution of session keys. A KDC is also considered as a special type of an authentication server in the following discussions.
- 2) Session key: information that enables two systems to establish a secured session.
- 10 Session keys have limited life span. Thus, if a secured session is not established within a certain period of time, a new session key is needed.
- 3) Kerberos client: initiates key distribution from the KDC and then uses the distributed session key to initiate a session with a peer.
- 4) Kerberos server: the peer system with which the Kerberos client wishes to establish a secured session.
- 15 5) Ticket: a Kerberos data structure that grants access of the Kerberos client to the Kerberos server.
- 6) Authenticator: a Kerberos data structure that Kerberos client uses to authenticate itself to a Kerberos server and also to challenge the Kerberos server to authenticate itself to the Kerberos client.

- 7) Response: a Kerberos data structure that the Kerberos server uses to authenticate itself to the Kerberos client.

Figure 2 illustrates one embodiment of the present invention or secured wireless roaming system (hereinafter SWRS) 200. SWRS 200 comprises one or 5 more specially configured wireless stations, such as wireless station 202, at least two specially configured access points, such as access points 206 and 208 and authentication server 210. Access points 206 and 208 are coupled to authentication server 210 via wired network 212 and are further coupled to wireless station 202 via wireless network 204. Authentication server 212 is responsible for maintaining and 10 providing security information and safeguarding the integrity of wired network 212 and wireless network 204. The interactions among access points 206 and 208, wireless station 202 and authentication server 212 for creating a secured roaming environment will be discussed with examples in the subsequent section that details the operations of SWRS 200.

15 Figure 3(a) illustrates a block diagram of one embodiment of wireless station 202. Wireless station 202 comprises control unit 300, transmitter 302, receiver 304, filter 306 and antenna 308. Control unit 300 is mainly responsible for, but not limited to, preparing data for transmission and consuming received data. One embodiment of control unit 300 includes two functional blocks:
20 encryption/decryption engine 314 and authentication protocol engine 316. An

alternative embodiment of control unit 300 may also incorporate a frequency channel selector to dynamically choose an appropriate frequency channel for wireless station 202. Encryption/decryption engine 314 encrypts data that wireless station 202 transmits and decrypts data that wireless station 202 receives with appropriate keys.

- 5 Additionally, authentication protocol engine 316 contains procedures for wireless station 202 to adhere to in order to further protect the overall integrity of wireless network 204 and wired network 212. Specific examples of the mentioned authentication procedures will be provided in the subsequent section.

Transmitter 302 and receiver 304 share antenna 308. On receive path 310, 10 filter 306 filters out signals received by antenna 308 that are outside of a predetermined frequency range. Receiver 304 is then responsible for extracting data from the filtered signals and passing the resulting data to control unit 300. On transmit path 312, control unit 300 sends prepared data to transmitter 302. Transmitter 302 modulates the prepared data with a carrier of proper frequency and 15 sends the modulated signal to filter 306. Filter 306 again eliminates spurious signal outside of the desired frequency range before transmitting the final filtered signal through antenna 308.

Figure 3(b) demonstrates a block diagram of one embodiment of access point 206 (or access point 208). Similar to wireless station 202, access point 206 also has 20 control unit 318, transmitter 320, receiver 322, filter 324 and antenna 326. Its

control unit 318 has encryption/decryption engine 324 and authentication protocol engine 326 that perform the same functions for access point 206 as encryption/decryption engine 314 and authentication protocol engine 316 do for wireless station 202. In addition, access point 206 has wired-network connection 5 interface 328 to communicate with wired network 212 as shown in Figure 2.

OPERATIONS OF A WIRELESS STATION AND ACCESS POINTS
IN A SECURED WIRELESS ROAMING SYSTEM

One specific embodiment of SWRS 200 mainly applies the Kerberos 10 protocol to secure communications among wireless station 202 and access points 206 and 208. In other words, authentication protocol engine 316 (Figure 3(a)) of wireless station 202 and authentication protocol engine 336 (Figure 3(b)) of access points 206 and 208 are specially configured to execute authentication procedures and to handle data structures specified by the Kerberos protocol. However, these 15 mentioned authentication protocol engines 316 and 336 also perform tasks that are either absent or distinct from the Kerberos protocol.

Figure 4 describes a flow chart of one process that one embodiment of wireless station 202 follows. This figure assumes the following: 1) authentication server 210 as shown in Figure 2 is the KDC; 2) wireless station 202 does not yet 20 have the session key to set up a secured session with access point 206, or session_key₂₀₆; 3) wireless station 202 is currently in the coverage area of access

point 206 and will “roam” in the coverage area of access point 208; 4) access points 206 and 208 share one group identification, ID_g ; and 5) the session key for wireless station 202 to establish a secured session with access point 208 is denoted as $session_key_{208}$.

- 5 In conjunction with Figures 2 and 3, instead of acting like a Kerberos client as in a typical application of the Kerberos protocol, authentication protocol engine 316 instructs wireless station 202 to behave as a Kerberos server and provides access point 208 with its identity information in block 400. Then authentication protocol engine 316 waits to respond to access point 206’s attempt to establish a secured
- 10 session using the newly obtained $session_key_{206}$ in block 402. A session is considered secured when wireless station 202 and access point 206 complete their mutual authentication within the lifetime of $session_key_{206}$. After authentication protocol engine 316 confirms that a secured session has been established, wireless station 202 obtains ID_g from access point 206. ID_g enables wireless station 202 to
- 15 access all the access points that share the same ID_g , such as access point 208.

- However, wireless station 202 cannot proceed to establish a secured session with access point 208 unless it has another valid session key, or $session_key_{208}$. As wireless station 202 moves into the coverage area of access point 208, authentication protocol engine 316 switches wireless station 202’s role back to being a Kerberos client and requests for $session_key_{208}$ from authentication server 210. It is important

to note that in a typical application of the Kerberos protocol, a Kerberos client needs to have the identity information of a peer system prior to initiating a session with such a system. In contrast, one embodiment of wireless station 202 simply uses session_key₂₀₈ and ID_g to initiate a session with access point 208.

- 5 Figure 5 illustrates a flow chart of one process that one embodiment of access point 206 (Figure 2) follows. This figure also relies on the same five assumptions described above. In parallel to the discussion for wireless station 202 above, authentication protocol engine 336 instructs access point 206 to behave as a Kerberos client instead of a Kerberos server. Thus, access point 206 initiates session
10 key distribution from authentication server 210 and attempts to establish a secured session with wireless station 202 using session_key₂₀₆ in block 500. After a secured session has been established in block 502, authentication protocol engine 336 provides wireless station 202 with ID_g in block 504.

- Authentication protocol engine 336 then dictates access point 206 to serve as
15 a proxy, or a relay agent, for wireless station 202. As a result, when access point 206 receives a session key request message, such as a ticket request message, from wireless station 202, encryption/decryption engine 334 decrypts the message and authentication protocol engine 336 relays the decrypted message to authentication server 210 in block 506. Similarly, authentication protocol engine 336 also relays
20 session_key₂₀₈ from authentication server 210 to wireless station 202 after the

session key becomes available. However, before the actual relay occurs, authentication protocol engine 336 appends certain information to session_key₂₀₈ to set the lifetime of the session key in block 508. In one embodiment, authentication protocol engine 336 selects and appends the current time of day, T, and a random number, N, to the session key.

In addition to the block diagrams as shown in Figures 2, 3(a) and 3(b) and flow charts as shown in Figures 4 and 5, the following tables further demonstrate implementation details of one embodiment of SWRS 200. Phase 1 corresponds to blocks 400, 402 and 404 as illustrated in Figure 4 and blocks 500, 502 and 504 as illustrated in Figure 5. Phase 2 corresponds to blocks 408, 506 and 508. At last, phase 3 corresponds to block 410.

Phase 1:

Actions	Explanations
Wireless station 202 → access point 206: ID_w	Wireless station 202 sends its identity information to access point 206.
Access point 206 → KDC: $ID_{ap\ 206}$, ID_w , $N_{ap\ 206}$	In addition to the identity information of access point 206 and wireless station 202, access point 206 also creates and sends a randomly generated number, $N_{ap\ 206}$, to KDC. This message that access point 206 sends to KDC is also referred to as the <i>ticket request message</i> .
KDC → access point 206: $E(K_w; K_{206}, ID_{ap\ 206}, L_{ap\ 206})$, $E(K_{ap}; K_{206}, N_{ap\ 206}, L_{ap\ 206}, ID_w)$ Note 1: The notation, $E(K, ***)$, means that *** is encrypted using encryption key K.	After KDC generates session key, K_{206} , KDC encrypts the session key with encryption keys of wireless station 202, K_w , and of access point 206, K_{ap} , and sends the encrypted messages to access point 206. These messages are also referred to as the <i>ticket granting message</i> . Encryption/decryption engine 334 of access

<p>Note 2: Session key, K_{206}, has a lifetime of $L_{ap\ 206}$.</p>	<p>point 206 deciphers part of the ticket granting message using the encryption key, K_{ap}, that it already has knowledge of and passes on the decrypted message to authentication protocol engine 336.</p> <p>Authentication protocol engine 336 proceeds to verify the value of $N_{ap\ 206}$ to ensure that the integrity of the information from KDC has not been compromised.</p>
<p>Access point 206 → wireless station 202: $E(K_w; K_{206}, ID_{ap\ 206}, L_{ap\ 206}, T_1)$</p> <p>Note: T_1 represents the time that access point 206 issues this challenge message.</p>	<p>Authentication protocol engine 336 of access point 206, as has been discussed before, has access point 206 act as a Kerberos client and sends its targeted Kerberos server, wireless station 202, a challenge message. A challenge message includes a ticket and an authenticator. In this case, the ticket is $E(K_w; K_{206}, ID_{ap\ 206}, L_{ap\ 206})$, and the authenticator is $E(K_{206}; ID_{ap\ 206}, T_1)$.</p>

Wireless station 202 → access point 206: $E(K_{206}; T_1)$	Wireless station 202 has from time T_1 to $T_1 + L_{ap\ 206}$ to authenticate itself to access point 206 by sending this response message, $E(K_{206}; T_1)$, to access point 206.
Access point 206 → wireless station 202: $E(K_{206}; ID_g)$	Access point 206 shares the group identity information with wireless station 202.

Phase 2

Actions	Explanations
Wireless station 202 → access point 206: $E(K_{206}; ID_w, ID_g, N_w)$ Note: N_w is a random number that wireless station 202 generates.	As has been mentioned in prior sections, wireless station 202 has changed back to being a Kerberos client. It generates and sends a ticket request message to access point 206 secured by session key, K_{206} .
Access point 206 → KDC: ID_w, ID_g, N_w	Access point 206 serves as a proxy for wireless station 202.
$KDC \rightarrow$ access point 206: $E(K_g; K_{208}, ID_w, L_{ap\ 208}), E(K_w; K_{208}, N_w, L_{ap\ 208}, ID_g)$	KDC responds to the ticket request message with a ticket granting message.

<p>Note: KDC creates a second session key, K_{208}, to allow wireless station 202 to establish a secured session with access point 208. It is important to emphasize that wireless station 202 relies on ID_g and does not need to depend on the identity information of access point 208 to set up the secured session. As a result, wireless station 202 avoids executing the same authentication sequences with access point 208 as it does with access point 206 and shortens the time required to establish the secured session with access point 208.</p>	
<p>Access point 206 → KDC: $E(K_{206}; E(K_g; K_{208}, ID_w, L_{ap\ 208}), E(K_w; K_{208}, N_w, L_{ap\ 208}, ID_g), T_2, E(K_g; N, ID_w, T_2))$</p> <p>Note: Wireless station 202 may execute the phase 2 protocol at any moment during</p>	<p>Access point 206 selects a time to be T_2, selects a random number N and appends T_2 and $E(K_g; N, ID_w, T_2)$ to the ticket granting message in order to enforce the lifetime of $session_key_{208}$. This prevents wireless station 202 from specifying an</p>

the time from T_1 to T_1+L_{206} .	unauthorized value for T_2 .
--	--------------------------------

Phase 3

Actions	Explanations
Wireless station 202 → access point 208: $ID_w, E(K_w; K_{208}, N_w, L_{208}, ID_g), E(K_{208};$ $ID_w, T_2), E(K_g; N, ID_w, T_2)$	With the information that access point 208 receives, it can verify the identity of wireless station 202 and determine the validity period of session_key ₂₀₈ (i.e. from T_2 to $T_2 + L_{208}$).
Access point 208 → wireless station 202: $E(K_{208}; ID_g), E(K_{208}; N', ID_w)$	The encrypted payload, $E(K_{208}; N', ID_w)$, protects wired network 212 against replay attacks. In other words, because access point 208 keeps generating new N's, wireless station 202 could rely on the varying N's to detect attempts to replay messages from access point 208.
Wireless station 202 → access point 208: $E(K_{208}; N')$	Wireless station 202 proves that it indeed has session_key ₂₀₈ .

Thus, a method and an apparatus for establishing secured roaming have been disclosed. Although the secured wireless roaming system has been described particularly with reference to the figures, one with ordinary skill in the art may further divide or combine the functionality of its functional blocks. For example, an
5 ordinarily skilled artisan may combine encryption/decryption engine 314 and authentication protocol engine 316 into one integrated component. Finally, despite the detailed discussion on Kerberos protocol, one of ordinary skill in the art could employ other authentication protocols without departing from the spirit and scope of the present invention.

CLAIMS

What is claimed is:

1. A method for establishing secured roaming among a wireless station, a first and a second access points, comprising:
 - a. the first access point requesting a first ticket from an authentication server and using the first ticket to establish a first secured session with the wireless station; and
 - b. in response to a second ticket request from the wireless station through the first secured session, the first access point forwarding the second ticket request to the authentication server and relaying a resulting second ticket from the authentication server to the wireless station.
2. The method according to claim 1, the method further comprises: applying the second ticket and a group identity shared by the first and the second access points to establish a second secured session between the wireless station and the second access point.
3. The method according to claim 1, the method further comprises:
 - a. the authentication server dynamically generating a first and a second session keys to include in the first and the second tickets, respectively;

and

- b. the authentication server encrypting the first and the second tickets with a first and a second encryption keys.
4. The method according to claim 3, the first and the second session keys have limited lifetime.
5. The method according to claim 3, the method further comprises:
 - a. the first access point appending application specific information to the second ticket to formulate a combined message; and
 - b. the first access point encrypting the combined message with the first session key.
6. The method according to claim 5, the application specific information further comprises the first access point's selected time and random number.
7. An access point in a secured wireless roaming system, comprising:
 - a. an antenna;
 - b. a filter coupled to the antenna;
 - c. a receiver and a transmitter coupled to the filter; and

- d. a control unit coupled to the receiver and the transmitter and coupled to a wired-network connection interface, wherein the control unit further comprises an authentication protocol engine that
- i. requests a first ticket from an authentication server and uses the first ticket to establish a first secured session with a wireless station; and
 - ii. in response to a second ticket request from the wireless station through the first secured session, forwards the second ticket request to the authentication server and relays a resulting second ticket from the authentication server to the wireless station.
8. The access point according to claim 7, the control unit further comprises: an encryption/decryption engine to decrypt the second ticket request before the authentication protocol engine forwards the second ticket request.
9. The access point according to claim 7, wherein the authentication server further:
- a. dynamically generates a first and a second session keys to include in the first and the second tickets, respectively; and

- b. encrypts the first and the second tickets with a first and a second encryption keys.
10. The access point according to claim 9, the first and the second session keys have limited lifetime.
11. The access point according to claim 8, further comprises:
- the authentication protocol engine to append application specific information to the second ticket to formulate a combined message; and
 - the encryption/decryption engine to encrypt the combined message with the first session key.
12. The access point according to claim 11, the application specific information further comprises the access point's selected time and random number.
13. A wireless station in a secured wireless roaming system, comprising:
- an antenna;
 - a filter coupled to the antenna;
 - a receiver and a transmitter coupled to the filter; and
 - a control unit coupled to the receiver and the transmitter, wherein the

control unit further comprises an authentication protocol engine that requests a second ticket from an authentication server via an access point after having used a first ticket to establish a first secured session with the access point.

14. The wireless station according to claim 13, comprising:
the authentication protocol engine to apply the second ticket and a group identity shared by the first and a second access points to establish a second secured session with the second access point.

15. A secured wireless roaming system, comprising:
a wired medium;
a wireless medium;
an authentication server coupled to the wired medium;
a wireless station coupled to the wireless medium; and
an access point coupled to the wireless medium and the wired medium,
wherein the access point comprises:
 - i. a first control unit, comprising a first authentication protocol engine to request a first ticket from the authentication server and use the first ticket to establish a first secured session with the

- wireless station; and
- ii. in response to a second ticket request from the wireless station through the first secured session, to forward the second ticket request to the authentication server and relays a resulting second ticket from the authentication server to the wireless station.
16. The secured wireless roaming system according to claim 15, wherein the wireless station further comprises:
a second authentication protocol engine to apply the second ticket and a group identity shared by the first and a second access points to establish a second secured session with the second access point.
17. The secured wireless roaming system according to claim 15, the first control unit further comprises:
an encryption/decryption engine to decrypt the second ticket request before the authentication protocol engine forwards the second ticket request.
18. The secured wireless roaming system according to claim 15, wherein the authentication server further:
a. dynamically generates a first and a second session keys to include in the

DO NOT PUBLISH

first and the second tickets, respectively; and

- b. encrypts the first and the second tickets with a first and a second encryption keys.

19. The secured wireless roaming system according to claim 17, the first and the second session keys have limited lifetime.

20. The secured wireless roaming system according to claim 17, further comprising:

- a. the first authentication protocol engine to append application specific information to the second ticket to formulate a combined message; and
- c. the first encryption/decryption engine to encrypt the combined message with the first session key.

21. The access point according to claim 20, the application specific information further comprises the access point's selected time and random number.

ABSTRACT OF THE DISCLOSURE

A method and an apparatus for establishing secured roaming among wireless devices are disclosed. In one embodiment, a first access point requests a first ticket from an authentication server and uses that first ticket to establish a first secured session with a wireless station. In response to a second ticket request from the wireless station through the first secured session, the first access point forwards the second ticket request to the authentication server and also relays a resulting second ticket from the authentication server back to the wireless station.

5

00000000000000000000000000000000

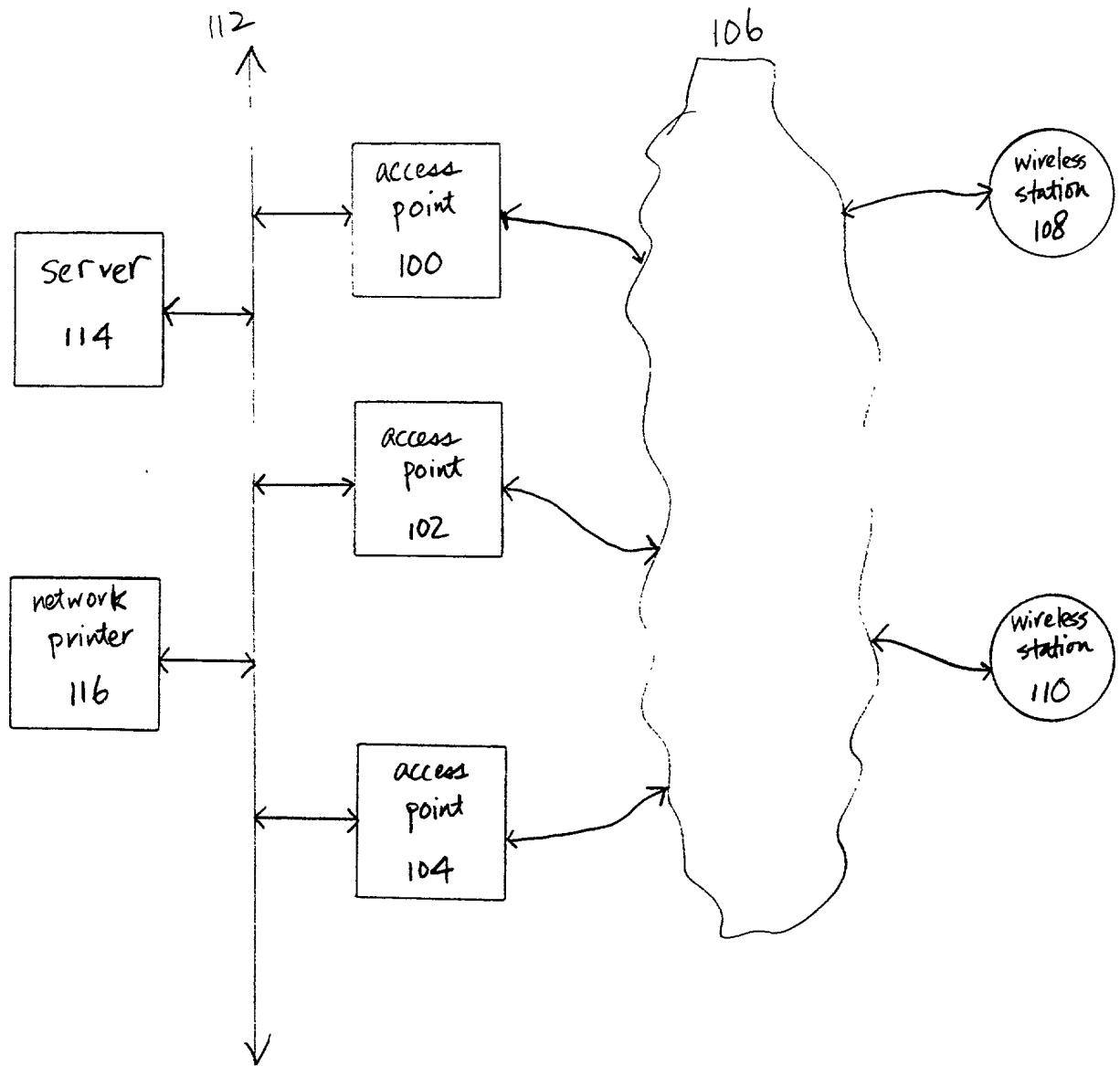


Figure 1 (prior art)

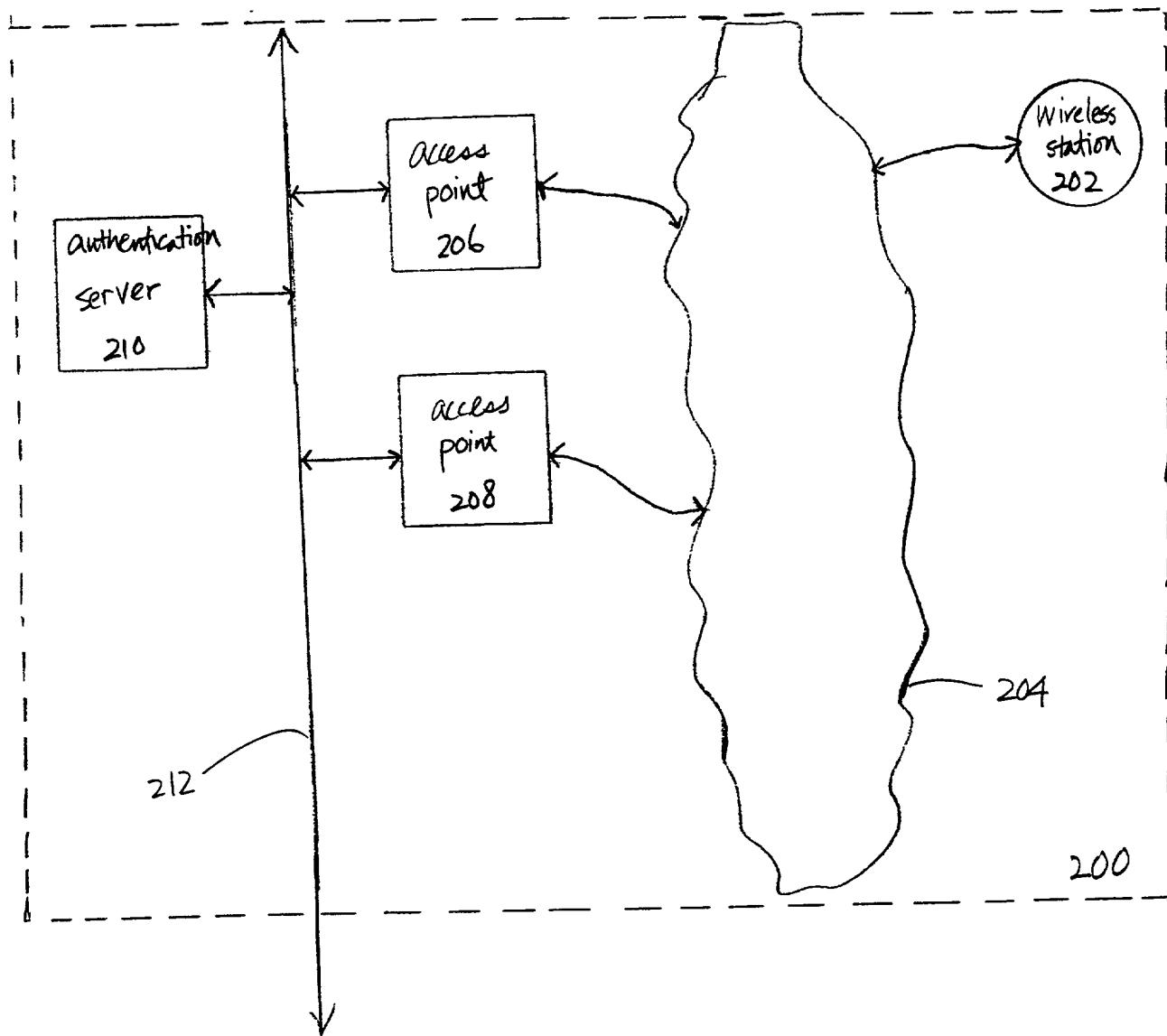


Figure 2

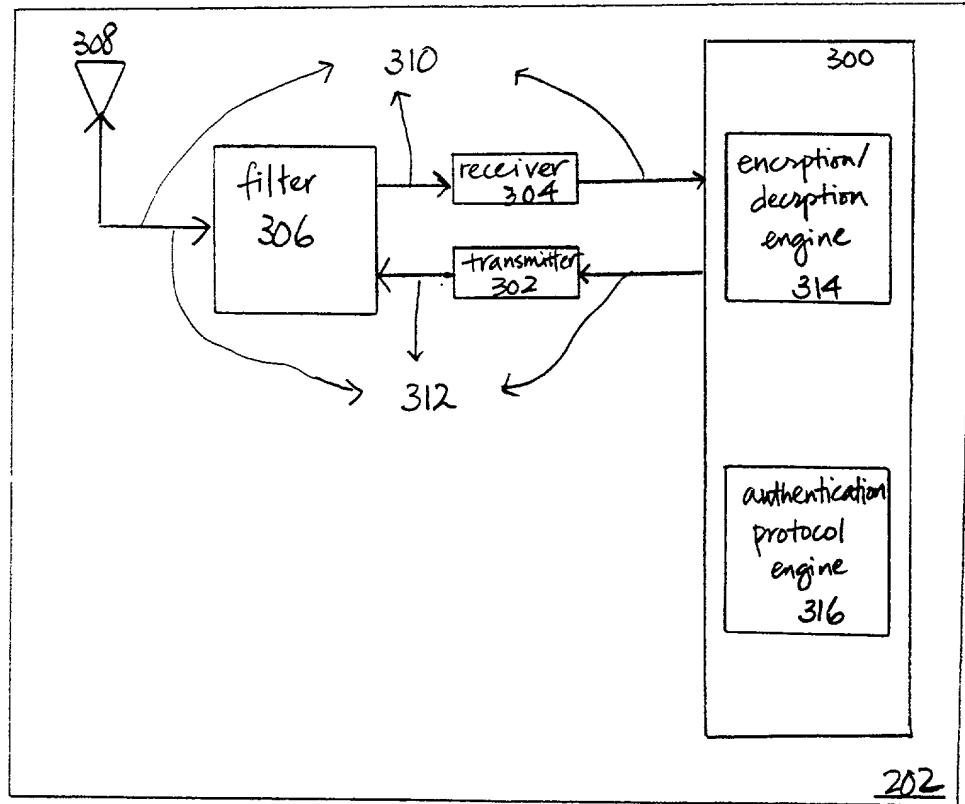


Figure 3(a)

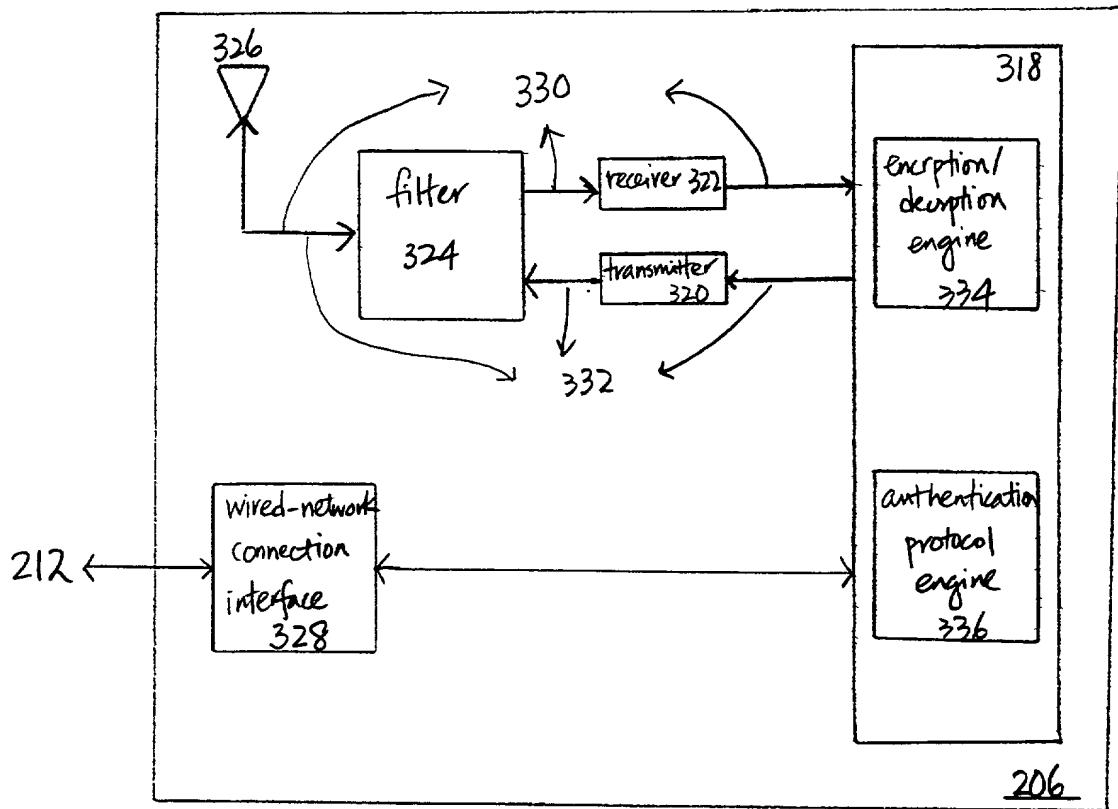


Figure 3(b)

0016220000000000

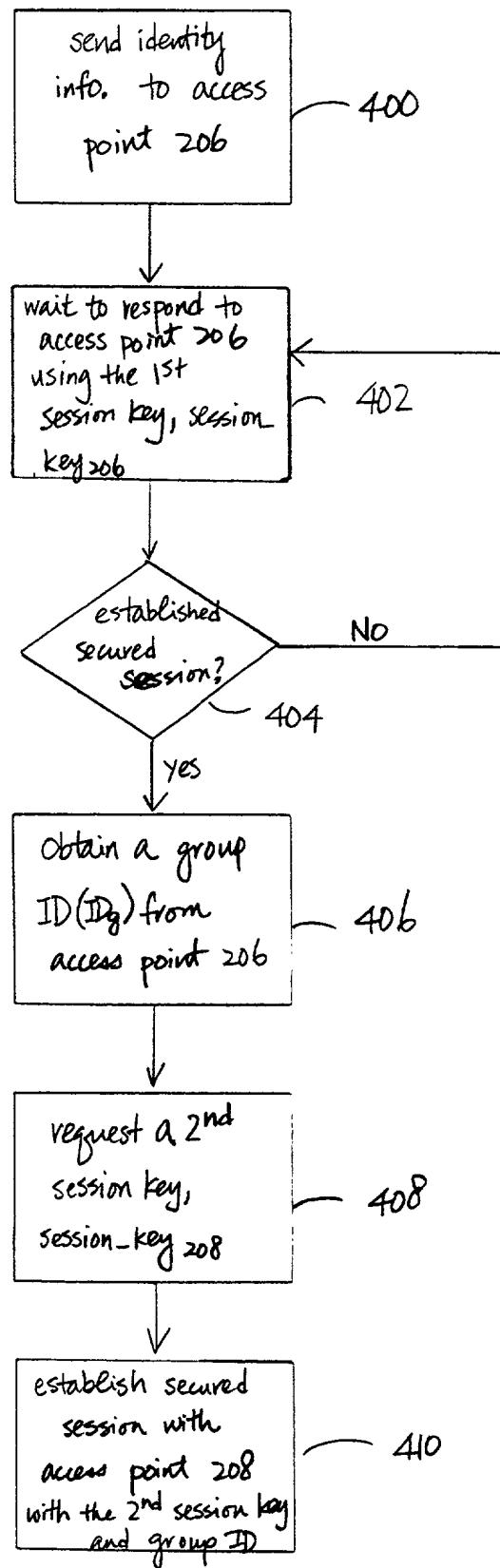


Figure 4

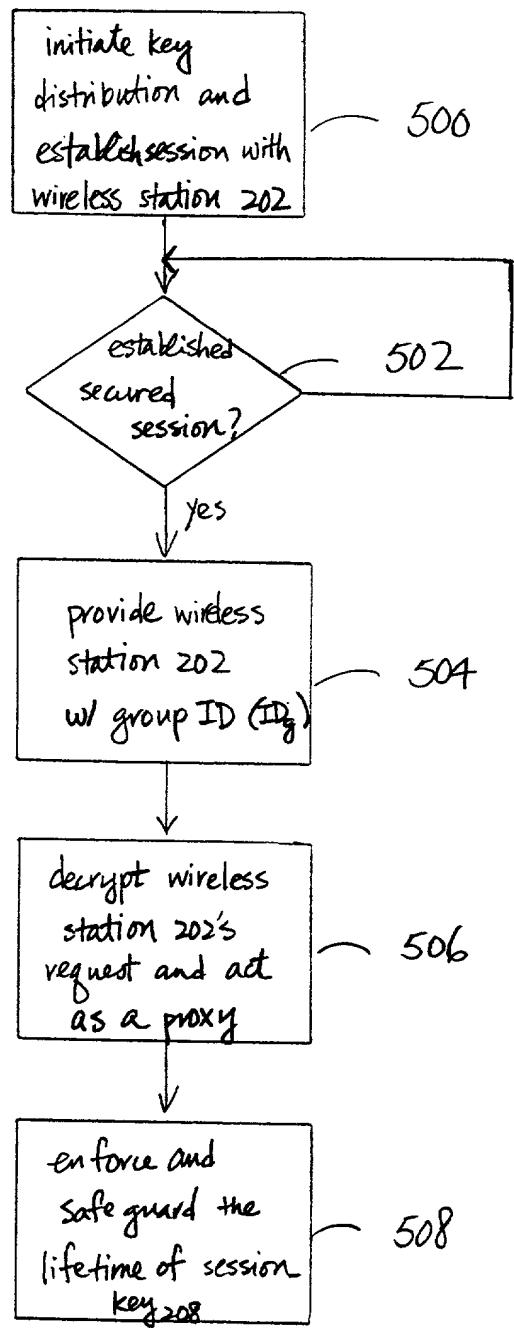


Figure 5

**DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION
(FOR INTEL CORPORATION PATENT APPLICATIONS)**

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below, next to my name.

I believe I am the original, first, and sole inventor (if only one name is listed below) or an original, first, and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

TECHNIQUE TO ESTABLISH WIRELESS SESSION KEYS SUITABLE FOR ROAMING
the specification of which

XX is attached hereto.
— was filed on (MM/DD/YYYY) _____ as
United States Application Number _____
or PCT International Application Number _____
and was amended on (MM/DD/YYYY) _____.
(if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment referred to above. I do not know and do not believe that the claimed invention was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof or more than one year prior to this application, that the same was not in public use or on sale in the United States of America more than one year prior to this application, and that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months (for a utility patent application) or six months (for a design patent application) prior to this application.

I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d), of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

<u>Prior Foreign Application(s)</u>			<u>Priority Claimed</u>
(Number)	(Country)	(Foreign Filing Date - MM/DD/YYYY)	Yes No
(Number)	(Country)	(Foreign Filing Date - MM/DD/YYYY)	Yes No
(Number)	(Country)	(Foreign Filing Date - MM/DD/YYYY)	Yes No

I hereby claim the benefit under Title 35, United States Code, Section 119(e) of any United States provisional application(s) listed below:

<u>Application Number</u>	<u>(Filing Date – MM/DD/YYYY)</u>
<u>Application Number</u>	<u>(Filing Date – MM/DD/YYYY)</u>

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

<u>Application Number</u>	<u>(Filing Date – MM/DD/YYYY)</u>	<u>Status -- patented, pending, abandoned</u>
<u>Application Number</u>	<u>(Filing Date – MM/DD/YYYY)</u>	<u>Status -- patented, pending, abandoned</u>

I hereby appoint the persons listed on Appendix A hereto (which is incorporated by reference and a part of this document) as my respective patent attorneys and patent agents, with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

Send correspondence to _____, BLAKELY, SOKOLOFF, TAYLOR &
(Name of Attorney or Agent)
ZAFMAN LLP, 12400 Wilshire Boulevard 7th Floor, Los Angeles, California 90025 and direct
telephone calls to _____, (408) 720-8300.
(Name of Attorney or Agent)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole/First Inventor Jesse R. Walker _____

Inventor's Signature _____ Date _____

Residence Portland, Oregon _____ Citizenship U.S.A. _____
(City, State) _____ (Country) _____

Post Office Address 10992 NW Appellate Way _____
Portland, Oregon 97229 _____

Full Name of Second/Joint Inventor _____

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____
(City, State) _____ (Country) _____

Post Office Address _____

Full Name of Third/Joint Inventor _____

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____
(City, State) _____ (Country) _____

Post Office Address _____

Full Name of Fourth/Joint Inventor _____

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____
(City, State) (Country)

Post Office Address _____

Full Name of Fifth/Joint Inventor _____

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____
(City, State) (Country)

Post Office Address _____

Full Name of Sixth/Joint Inventor _____

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____
(City, State) (Country)

Post Office Address _____

Full Name of Seventh/Joint Inventor _____

Inventor's Signature _____ Date _____

Residence _____ Citizenship _____
(City, State) (Country)

Post Office Address _____

APPENDIX A

William E. Alford, Reg. No. 37,764; Farzad E. Amini, Reg. No. 42,261; William Thomas Babbitt, Reg. No. 39,591; Carol F. Barry, Reg. No. 41,600; Jordan Michael Becker, Reg. No. 39,602; Lisa N. Benado, Reg. No. 39,995; Bradley J. Bereznak, Reg. No. 33,474; Michael A. Bernadicou, Reg. No. 35,934; Roger W. Blakely, Jr., Reg. No. 25,831; R. Alan Burnett, Reg. No. 46,149; Gregory D. Caldwell, Reg. No. 39,926; Andrew C. Chen, Reg. No. 43,544; Thomas M. Coester, Reg. No. 39,637; Donna Jo Coningsby, Reg. No. 41,684; Florin Corie, Reg. No. 46,244; Dennis M. deGuzman, Reg. No. 41,702; Stephen M. De Clerk, Reg. No. 46,503; Michael Anthony DeSanctis, Reg. No. 39,957; Daniel M. De Vos, Reg. No. 37,813; Sanjeet Dutta, Reg. No. 46,145; Matthew C. Fagan, Reg. No. 37,542; Tarek N. Fahmi, Reg. No. 41,402; George Fountain, Reg. No. 37,374; James Y. Go, Reg. No. 40,621; James A. Henry, Reg. No. 41,064; Libby N. Ho, Reg. No. 46,774; Willmore F. Holbrow III, Reg. No. 41,845; Sheryl Sue Holloway, Reg. No. 37,850; George W Hoover II, Reg. No. 32,992; Eric S. Hyman, Reg. No. 30,139; William W. Kidd, Reg. No. 31,772; Sang Hui Kim, Reg. No. 40,450; Walter T. Kim, Reg. No. 42,731; Eric T. King, Reg. No. 44,188; George Brian Leavell, Reg. No. 45,436; Kurt P. Leyendecker, Reg. No. 42,799; Gordon R. Lindeen III, Reg. No. 33,192; Jan Carol Little, Reg. No. 41,181; Robert G. Litts, Reg. No. 46,876; Joseph Lutz, Reg. No. 43,765; Michael J. Mallie, Reg. No. 36,591; Andre L. Marais, under 37 C.F.R. § 10.9(b); Paul A. Mendonsa, Reg. No. 42,879; Clive D. Menezes, Reg. No. 45,493; Chun M. Ng, Reg. No. 36,878; Thien T. Nguyen, Reg. No. 43,835; Thinh V. Nguyen, Reg. No. 42,034; Dennis A. Nicholls, Reg. No. 42,036; Daniel E. Ovanezian, Reg. No. 41,236; Kenneth B. Paley, Reg. No. 38,989; Gregg A. Peacock, Reg. No. 45,001; Marina Portnova, Reg. No. 45,750; William F. Ryann, Reg. 44,313; James H. Salter, Reg. No. 35,668; William W. Schaal, Reg. No. 39,018; James C. Scheller, Reg. No. 31,195; Jeffrey Sam Smith, Reg. No. 39,377; Maria McCormack Sobrino, Reg. No. 31,639; Stanley W. Sokoloff, Reg. No. 25,128; Judith A. Szepesi, Reg. No. 39,393; Vincent P. Tassinari, Reg. No. 42,179; Edwin H. Taylor, Reg. No. 25,129; John F. Travis, Reg. No. 43,203; Joseph A. Twarowski, Reg. No. 42,191; Tom Van Zandt, Reg. No. 43,219; Lester J. Vincent, Reg. No. 31,460; Glenn E. Von Tersch, Reg. No. 41,364; John Patrick Ward, Reg. No. 40,216; Mark L. Watson, Reg. No. 46,322; Thomas C. Webster, Reg. No. 46,154; and Norman Zafman, Reg. No. 26,250; my patent attorneys, and Firasat Ali, Reg. No. 45,715; Justin M. Dillon, Reg. No. 42,486; Thomas S. Ferrill, Reg. No. 42,532; and Raul Martinez, Reg. No. 46,904, my patent agents, of BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, with offices located at 12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025, telephone (310) 207-3800, and Alan K. Aldous, Reg. No. 31,905; Edward R. Brake, Reg. No. 37,784; Ben Burge, Reg. No. 42,372; Jeffrey S. Draeger, Reg. No. 41,000; Cynthia Thomas Faatz, Reg. No. 39,973; John N. Greaves, Reg. No. 40,362; Seth Z. Kalson, Reg. No. 40,670; David J. Kaplan, Reg. No. 41,105; Peter Lam, Reg. No. 44,855; Charles A. Mirho, Reg. No. 41,199; Leo V. Novakoski, Reg. No. 37,198; Thomas C. Reynolds, Reg. No. 32,488; Kenneth M. Seddon, Reg. No. 43,105; Mark Seeley, Reg. No. 32,299; Steven P. Skabrat, Reg. No. 36,279; Howard A. Skaist, Reg. No. 36,008; Gene I. Su, Reg. No. 45,140; Calvin E. Wells, Reg. No. P43,256, Raymond J. Werner, Reg. No. 34,752; Robert G. Winkle, Reg. No. 37,474; Steven D. Yates, Reg. No. 42,242; and Charles K. Young, Reg. No. 39,435; my patent attorneys, of INTEL CORPORATION; and James R. Thein, Reg. No. 31,710, my patent attorney with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

APPENDIX B

Title 37, Code of Federal Regulations, Section 1.56 Duty to Disclose Information Material to Patentability

(a) A patent by its very nature is affected with a public interest. The public interest is best served, and the most effective patent examination occurs when, at the time an application is being examined, the Office is aware of and evaluates the teachings of all information material to patentability. Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability as defined in this section. The duty to disclosure information exists with respect to each pending claim until the claim is cancelled or withdrawn from consideration, or the application becomes abandoned. Information material to the patentability of a claim that is cancelled or withdrawn from consideration need not be submitted if the information is not material to the patentability of any claim remaining under consideration in the application. There is no duty to submit information which is not material to the patentability of any existing claim. The duty to disclosure all information known to be material to patentability is deemed to be satisfied if all information known to be material to patentability of any claim issued in a patent was cited by the Office or submitted to the Office in the manner prescribed by §§1.97(b)-(d) and 1.98. However, no patent will be granted on an application in connection with which fraud on the Office was practiced or attempted or the duty of disclosure was violated through bad faith or intentional misconduct. The Office encourages applicants to carefully examine:

- (1) Prior art cited in search reports of a foreign patent office in a counterpart application, and
 - (2) The closest information over which individuals associated with the filing or prosecution of a patent application believe any pending claim patentably defines, to make sure that any material information contained therein is disclosed to the Office.
- (b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made or record in the application, and
- (1) It establishes, by itself or in combination with other information, a prima facie case of unpatentability of a claim; or
 - (2) It refutes, or is inconsistent with, a position the applicant takes in:
 - (i) Opposing an argument of unpatentability relied on by the Office, or
 - (ii) Asserting an argument of patentability.

A prima facie case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

- (c) Individuals associated with the filing or prosecution of a patent application within the meaning of this section are:
- (1) Each inventor named in the application;
 - (2) Each attorney or agent who prepares or prosecutes the application; and
 - (3) Every other person who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application.
- (d) Individuals other than the attorney, agent or inventor may comply with this section by disclosing information to the attorney, agent, or inventor.